a3B1 cont

26. (New) A method as recited in claim 25, wherein the method is performed by a data storage apparatus data transmission comprising a transmission to a data storage device having a device address within the data storage apparatus, said storing comprises storing a data storage device encryption key, and said selecting comprises selecting the device encryption key when the transmission is to the storage device.

REMARKS

In the Office Action mailed September 24, 2002 the Examiner noted that claims 1-21 were pending, and rejected all claims. Claims 1-7 and 9-19 have been amended, claims 20 and 21 have been canceled, new claims 22-26 have been added and, thus, in view of the forgoing claims 1-19 and 22-26 remain pending for reconsideration which is requested. No new matter has been added. The Examiner's rejections are traversed below.

In the Office Action the Examiner rejected claims 1-5, 8, 9, 11, 12, 17, 18, 20, and 21 as anticipated by Kuroda and rejected claims 5-7, 11-16 and 19 as obvious over Kuroda and MIttra.

The present invention is designed to solve a problem associated with protecting data transmissions from a data transmission source. The data transmissions can be local transmissions, such as over a local area network or to a storage device, such as a data server, associated with the data source. Or the data transmissions can be global transmissions, such as over the Internet. In a global type transmission, it is typical to use a key common to a number of data sources, such as a public key. In the local type transmission, it is typical to use a private key between machines on a local area network or even a special device key when the transmission is to the associated storage device. A problem arises when the data source uses the wrong key to encrypt the data to be transmitted. The present invention is designed to solve this problem. The present invention selects the key to be used responsive to the destination of the data transmission (see figures 2 and 3 and the description thereof in the specification). This ensures that the correct key is used for the data transmission. This feature of selecting the key is emphasized in the independent claims.

In contrast, Kuroda involves data authentication where authentication information is used to verify that the data stored in a storage device is correct. The system solves a problem associated with the loss of a secret key that would allow the security of data to be lost. During operation, a first mutual authentication unit generates authentication information by encrypting data storage identification information and random information using a master key. This first mutual authentication information is transmitted to another electronic storage device. The first authentication unit receives second mutual authentication information and this information is decrypted and compared to see if it is correct, that is, to see if it matches the information sent. There is nothing in Kuroda that discusses selection keys based on the destination.

Mittra adds nothing to Kuroda with respect to the features of the invention discussed above.

It is submitted that the present claimed invention patentably distinguishes over the prior art and withdrawal of the rejection is requested.

It is submitted that the claims are not taught, disclosed or suggested by the prior art. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

If any further fees, other than and except for the issue fee, are necessary with respect to this paper, the U.S.P.T.O. is requested to obtain the same from deposit account number 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 12/24/2

By:
J. Randall Beckers
Registration No. 30,358

700 Eleventh Street, NW, Suite 500
Washington, D.C. 20001
(202) 434-1500

CERTIFICATE UNDER 37 CFR 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231

on December 24, 20 2002

STAAS & HALSEY

By: Regina Bennett

Date December 24, 2002

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

Please CANCEL claims 20 and 21.

Please AMEND the following claims:

1. (Once Amended) An electronic data storage apparatus for storing electronic data, comprising:

a key management unit [means for] managing an individual key unique to the electronic data storage apparatus to which said [means] management unit belongs, and a common key shared with other electronic data storage apparatuses[; and encryption means for], selecting the individual key when performing an [encrypting] encryption process on electronic data stored in the electronic data storage apparatus to which said management unit [means] belongs [using the individual key], and selecting the common key when performing the encryption [an encrypting] process [using the common key] or [with data verification on] when verifying electronic data transmitted to or received from another electronic data storage apparatus; and

an encryption unit performing the encryption process using the key selected by said key management unit.

2. (Once Amended) The apparatus according to claim 1, wherein said key management [means] unit manages a group key as the common key to be shared in a group of a plurality of electronic data storage apparatuses.

3. (Once Amended) The apparatus according to claim 1, wherein:

a main electronic data storage apparatus exists in the group;

said encryption [means] unit of said main electronic data storage apparatus generates an individual key of each electronic data storage apparatus in the group using an individual key of the apparatus to which said [means] management unit belongs; and

said generated individual key is distributed to each electronic data storage apparatus belonging to the group.

4. (Once Amended) The apparatus according to claim 2, wherein:

a main electronic data storage apparatus exists in the group;

said encryption [means] unit of said main electronic data storage apparatus generates a group key to be shared in the group using an individual key of the apparatus to which said [means] management unit belongs; and

said generated group key is distributed to each electronic data storage apparatus belonging to the group.

5. (Once Amended) The apparatus according to claim 2, wherein:

a main electronic data storage apparatus exists in the group;

said encryption [means] unit of said main electronic data storage apparatus generates a group key to be shared in the group with a key preliminarily assigned

as the individual key to said main electronic data storage apparatus associated with a new key externally specified; and

said generated group key is distributed to each electronic data storage apparatus belonging to the group.

6. (Once Amended) The apparatus according to claim 2, wherein:

a main electronic data storage apparatus exists in the group, and an electronic data storage and management apparatus for managing respective main electronic data storage apparatuses in a plurality of groups exists;

said encryption [means] unit of said electronic data storage and management apparatus generates an individual key of each of said main electronic data storage apparatuses using an individual key of the apparatus to which said [means] management unit belongs; and

said generated individual key is distributed to each of said main electronic data storage apparatuses.

7. (Once Amended) The apparatus according to claim 2, wherein said key management [means] unit manages, in addition to said group key as the common key, a public key for use in transmitting electronic data to and receiving it from an electronic data storage apparatus belonging to a group different from a group of the electronic data storage apparatus to which said [means] management unit belongs.

9. (Once Amended) The apparatus according to claim 1, wherein:

said encryption [means] unit generates the individual key with a key preliminarily set before use of the apparatus to which said [means] management unit belongs with a new externally specified key; and

said key management [means] unit manages the generated individual key.

10. (Once Amended) The apparatus according to claim 1, wherein said key management [means] unit manages, in addition to the individual key and the common key, a master key to be shared by all electronic data storage apparatuses.

11. (Once Amended) The apparatus according to claim 10, wherein:

said encryption [means] unit generates the individual key by encrypting information identifying the apparatus to which said [means] management unit belongs using the master key; and

said key management [means] unit manages the generated individual key.

12. (Once Amended) The apparatus according to claim 11, wherein:

a main electronic data storage apparatus exists in a group of a plurality of electronic data storage apparatuses;

said encryption [means] unit of said main electronic data storage apparatus generates a group key as the common key by encrypting information identifying the group using the generated individual key; and

said generated group key is distributed to each electronic data storage apparatus belonging to the group.

13. (Once Amended) The apparatus according to claim 1, wherein:

a hierarchical structure of electronic data storage apparatuses is designed as having a group of a plurality of electronic data storage apparatuses as one hierarchical level; and

said key management unit [means] manages a group key as the common key depending on [a] the hierarchical level of [a] the group containing the electronic data storage apparatus to which said [means] management unit belongs.

14. (Once Amended) The apparatus according to claim 13, wherein:

in the hierarchical structure of the electronic data storage apparatuses, an electronic data storage and management apparatus for managing electronic data storage apparatuses in a lower order group exists in a group at one level higher than the lower order group;

said encryption [means] unit of said electronic data storage and management apparatus generates a group key for the lower order group using the individual key of the apparatus to which said [means] management unit belongs; and

said generated group key is distributed to the electronic data storage apparatuses in the group at one level lower.

15. (Once Amended) A method of managing electronic data in an electronic data storage apparatus in a hierarchical structure having a group of a plurality of electronic data storage apparatuses as one hierarchical level, comprising [the steps of]:

[a transmitting] re-encrypting, by a first electronic data storage apparatus in one hierarchical level of the hierarchical structure, [re-encrypting] data[,] encrypted using an individual key which is unique to and stored in the apparatus, using a higher order group key corresponding to the hierarchical level, and transmitting the re-encrypted data to an electronic data storage and management apparatus for managing the electronic data storage apparatuses in a group at one hierarchical level lower;

verifying, by said electronic data storage and management apparatus for managing a lower group of electronic data storage apparatuses, [verifying] the received data using the higher order group key[;] , re-encrypting the received [electronic] data using the lower order group key corresponding to one hierarchical level lower if the [electronic] received data is correct as a result of the verification, and transmitting the received data to a second [receiving] electronic data storage apparatus in the group at one level lower; and

[said receiving] verifying, by the second electronic data storage apparatus, [verifying] the received data using the lower order group key,[; and] re-encrypting [and storing] the received data using an individual key unique to the second electronic data storage apparatus if the electronic data is correct as a result of the verification, and storing the re-encrypted received data.

16. (Once Amended) A method of managing electronic data in an electronic data storage apparatus in a hierarchical structure having a group of a plurality of electronic data storage apparatuses as one hierarchical level, comprising [the steps of]:

re-encrypting, by a first [a transmitting] electronic data storage apparatus in one hierarchical level of the hierarchical structure, [re-encrypting] data[,] encrypted using an individual key which is unique to and stored in the first electronic data storage apparatus, using a lower order group key corresponding to the hierarchical level, and transmitting the re-encrypted data to a lower order group electronic data storage and management apparatus for managing the electronic data storage apparatuses in the group;

verifying, by said electronic data storage and management apparatus for managing a lower group of electronic data storage apparatuses, [verifying] the received data using the lower order group key,[;] re-encrypting the received [electronic] data using the higher order group key corresponding to one hierarchical level higher if the electronic data is correct as a result of the verification, and transmitting the data to a receiving electronic data storage apparatus in the group at one level higher;

verifying, by the second [said receiving] electronic data storage apparatus, [verifying] the received data using the higher order group key[; and], re-encrypting [and storing] the received data using an individual key unique to the second electronic data storage apparatus if the electronic data is correct as a result of the verification, and storing the re-encrypted received data.

17. A method of processing [storing] electronic data [in an electronic data storage apparatus for storing the electronic data], comprising the [steps of]:

storing in a storage unit an individual key unique to an electronic data storage apparatus for storing electronic data and a common key shared with another electronic data storage apparatus;

selecting the common key stored in the storage unit as a key to be used when communicating electronic data [using a common key shared with other electronic data storage apparatuses]; [and]

selecting the individual key to be used when performing an [encrypting] encryption process [using an individual key unique to an electronic data storage apparatus] on data to be stored in the electronic data storage apparatus; and

performing the communication process or encryption process using the selected key.

18. (Once Amended) The method according to claim 17, wherein;

said electronic data storage apparatus stores as the common key a group key shared in one group of a plurality of electronic data storage apparatuses;

[a transmitting] re-encrypting, by a first electronic data storage apparatus, [transmits] electronic data, encrypted using the individual key and stored in the first electronic data storage apparatus, [after re-encrypting] using the group key [the data stored in the apparatus and encrypted using the individual key; a receiving] , and transmitting the data to a second electronic data storage apparatus [verifies] ; and

verifying by the second electronic data storage apparatus, the received electronic data using the group key[; and], re-encrypting the received electronic data using the individual key when the electronic data is correct according to [a] the result of the verification[, said electronic data is re-encrypted using the individual key and stored] , and storing the re-encrypted received data.

19. (Once Amended) The method according to claim 17, wherein:

said electronic data storage apparatus belonging to a group of electronic data storage apparatuses stores as the common key a public key of an electronic data storage apparatus belonging to another group of a plurality of electronic data storage apparatuses;

re-encrypting by a first [a transmitting] electronic data storage apparatus, [transmits] electronic data , encrypted using individual key and stored in the first electronic data storage apparatus [after re-encrypting] using the public key [the data stored in the apparatus and encrypted using the individual key; a receiving] and transmitting data to a second electronic data storage apparatus ; and

verifying by the second electronic data storage apparatus [verifies] the received electronic data using a private key which is a pair [to] member with the public key[; and] , re-encrypting the received electronic data using the individual key when the electronic data is correct according to [a] the result of the verification[, said electronic data is re-encrypted using the individual key and stored] , and storing the re-encrypted received data.

Please ADD the following claims:

22. (New) An electronic data storage apparatus for storing electronic data, comprising:

key management means for managing an individual key unique to the electronic data storage apparatus to which said key management means belongs, and a common key shared with other electronic data storage apparatuses, selecting the individual key when performing an encrypting encryption process on electronic data stored in the electronic data storage apparatus to which said means belongs, and selecting the common key when performing an encryption process or when verifying electronic data transmitted to or received from another electronic data storage apparatus; and

encryption means for performing the encryption process using the key selected by said key management unit.

23. (New) A computer-readable storage medium for storing the program which directs a computer to process electronic data, comprising of:

storing in a storage unit an individual key unique to an electronic data storage apparatus for storing electronic data and a common key shared with another electronic data storage apparatus;

selecting the common key stored in the storage unit as a key to be used when communicating electronic data;

selecting the individual key as a key to be used when performing an encryption process on data to be stored in the electronic data storage apparatus; and

performing the communication process or the encryption process using the selected key.

24. (New) A method of data transmission for a local environment and a global environment, comprising:

storing a local encryption key for the local environment and storing a global key for the global environment;

receiving data to be transmitted along with an environment indicator indicating the environment of the data transmission;

selecting one of the local and global encryption keys responsive to the indicator;

encrypting the data with the selected one of the keys; and

transmitting the encrypted data.

25. (New) A method as recited in claim 24, wherein the local environment comprises a local area network, the global environment comprises the internet, and the indicator is an address of the data transmission where a local area address indicates the local environment.

26. (New) A method as recited in claim 25, wherein the method is performed by a data

storage apparatus data transmission comprising a transmission to a data storage device having a device address within the data storage apparatus, said storing comprises storing a data storage device encryption key, and said selecting comprises selecting the device encryption key when the transmission is to the storage device.